Remarks / Arguments

Claims 1-22 remain in the application, of which claims 1-21 stand rejected and claim 22 stands allowed.

Claim 1 has been amended to clarify that data transmitted over a number of microprocessor buses is randomly sampled via inputs to the number of MISRs. Support for this amendment is found, at least, in paragraphs [0017], [0021] and [0038].

Claims 3-7 and 12 have been amended to conform to the amendment of claim 1.

Claim 20 has been amended to better state that which is being claimed.

None of the above amendments are believed to add new matter.

1. Rejection of Claims 1-21 Under 35 USC 101

Claims 1-21 stand rejected under 35 USC 101 as being directed to non-statutory subject matter. More specifically, the examiner asserts:

> Claims 1-21 recites [sic] a method of generating a random number according to a mathematical algorithm. In order for a method claims [sic] to be statutory, the claims must include a practical application that produces a useful, concrete, and tangible result. However, the claims merely recite a method of generating a random number based upon an algorithm. As guided, a claim that recites a computer implemented [sic] that solely calculates a mathematical formula or a computer medium that solely stores a mathematical formula is not statutory. Therefore, claims 1-21 are directed to non-statutory subject matter.

2/27/2006 Office Action, p. 2, section 5.

Applicant respectfully disagrees. To begin, it is noted that claims 1-21 are directed toward the generation of *random numbers*. That is, the claims are not directed toward simple implementation of an algorithm or mathematical formula,

but rather to a novel way to use MISRs (apparatus) and randomly sampled data transmitted over a number of microprocessor buses (apparatus) to generate random numbers. Unlike the application of a mathematical formula, there is no "right" answer to be obtained by applicant's claimed methods. In fact, the exact opposite is true, in that the purpose of applicant's methods is to generate "random numbers" that are so random in nature that an attacker cannot discern any sort of algorithm or mathematical formula that is used to generate the random numbers. A significant problem encountered in random number generators is that most of what occurs within computers, in nature, and elsewhere, is not random, but subject to being described and modeled by a mathematical formula. This is why the creation of a good random number generator is difficult, and why methods like those claimed by applicant are useful.

The practical applications for random numbers are well known in the art and include encryption keys and the like, as discussed in the background of the application (p.1, par. [0002]-[0009]). Many other applications (e.g., gaming, scientific studies) utilize random numbers as an input and would therefore benefit from the claims of the application.

Generation of random numbers is a process that is "limited to a practical application which produces a useful, tangible, and concrete result." *Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility* (undated), p. 33, line 3-4, quoting Diehr, 450 U.S. at 183-84, 209 USPQ at 6. Generation of a random number produces a 1) practical, especially in the encryption arts, 2) tangible, in that the result is a number and not an abstract concept and has a practical application, and 3) concrete *result*. Ibid, at p. 20, lines 6-8, quoting AT&T, 172 F.3d at 1358-59, 50 USPQ2d at 1452. A process for generating a random number is "concrete" if it "can be substantially repeatable or the process substantially produces the same result again." Ibid at p. 22, lines 8-9, quoting In re Swartz, 232 F.3d. 862, 864, 56 USPQ2d 173, 1704 (Fed. Cir. 2000). The "same result" criteria is met as each execution of the process produces a random number.

For at least the reasons presented above, applicant asks the Examiner to withdraw the rejection of claims 1-21 under 35 USC 101.

2. Rejection of Claims 1, 2, 7-16, 18, 20 and 21 Under 35 USC 102(b)

Claims 1, 2, 7-16, 18, 20 and 21 are rejected under 35 USC 102(b) as being anticipated by U.S. Pat. No. 5,416,783 to Broseghini et al (hereinafter, "Broseghini").

Regarding claim 1, the Examiner asserts:

> Re claim 1, Broseghini et al. discloses in Figures 1-9 a method of generating a random number (e.g., [Broseghini] col. 9 lines 41-44), comprising: retrieving values from a number of multiple input shift registers (MISRs)(e.g., [Broseghini] col. 9 lines 45-54 and col. 13 lines 47-56, steps 2 and 3) which are coupled to a number of microprocessor buses (e.g., [Broseghini] Figure 3 and col. 2 lines 14-28); and generating a random number which is based on the values retrieved from the number of MISRs (e.g., col. 10 lines 3-14).

Applicant respectfully disagrees. Claim 1, as amended, recites:

> A method of generating a random number, comprising:
> via inputs to a number of multiple input shift registers (MISRs), randomly sampling data transmitted over a number of microprocessor buses;
> retrieving values from the number of MISRs; and
> generating a random number which is based on the values retrieved from the number of MISRs.

The art of record fails to teach or reasonably suggest a number of MISRs having inputs that *sample* the data transmitted over a number of microprocessor buses. The values on a bus are highly random and can include data from a variety of sources, such as, cache accesses, disk accesses, user input (e.g., keystrokes), network traffic, and other data operations (*see*, page 1, par. [0016], of applicant's specificaiton).

In contrast to applicant's methods, in which a number of MISRs are effectively "seeded" by random samples of bus data, Broseghini requires a user to "load a desired SEED value into IY register 101" (col. 10, lines 62-63), and it is

this user-loaded SEED value that then forms the basis for generating a pseudo-random number.

For at least the reasons presented above, claim 1 is believed to be allowable. Claims 2, 7-16, 18, 20 and 21 are believed to be allowable, at least, for the reason that they provide further limitations on claim 1.

3. Conclusion

In summary, the art of record does not teach nor suggest the subject matter of applicant's claims 1-22. Claims 1-21 are therefore believed to be allowable, and accordingly, applicant respectfully requests the issuance of a Notice of Allowance.

Respectfully submitted,
DAHL & OSTERLOTH, L.L.P.

By: 

Gregory W. Osterloth
Reg. No. 36, 232
Tel: (303) 291-3204